Cybersecurity Preparedness

SELF-ASSESSMENT QUESTIONNAIRE

November 2022

(Version 1.2)

mhcc.maryland.gov

Toll Free: 1-877-245-1762
TTY Number: 1-800-735-2258
Fax: 410-358-1236

4160 Patterson Avenue
Baltimore, MD 21215

INTRODUCTION

Cybersecurity is essential for all businesses, including heath care provider organizations, such as practices, clinics, and health centers (herein referred to as organizations throughout), to prevent, detect, and respond to cyber threats and attacks.[1] Cybersecurity is not limited to just the technology systems that store and transmit patient data; it encompasses people and processes to make sure operations and security are working in tandem. Assessing cybersecurity preparedness helps ensure cyber threats are treated like any other disaster (e.g., fires, floods, outbreaks) and encompasses a review of preventative measures that protect patient privacy and safety and limit disruption to organization operations should a cyber-attack occur.

The Maryland Health Care Commission (MHCC), in collaboration with stakeholders, developed a *Cybersecurity Preparedness Self-Assessment Questionnaire* (questionnaire) to assist organizations with assessing cybersecurity. The questionnaire includes select elements from the National Institute of Standards and Technology (NIST)[2] Cybersecurity Framework (CSF).[3] The NIST CSF was developed through a collaborative process with experts in the federal government and private sector to create a set of standards, best practices, and recommendations for improving cybersecurity.[4] The five core functions of the NIST CSF include: Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC).[5] Each function has a list of categories and subcategories that define specific cybersecurity activities that should be performed continuously and concurrently. Users of the questionnaire are encouraged to review the NIST CSF at: nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

INSTRUCTIONS

The questionnaire consists of a series of self-evaluation statements intended to help users identify potential gaps in cybersecurity and prioritize areas for improvement. Statements are grouped by people, processes, and technology and reference the NIST CSF function, category, and subcategory and applicable page numbers in the NIST CSF (Version 1.1, April 2018). Click on the source for more information.[6] For each statement, select one of the following response options that most accurately reflects how you would categorize your organization's ability to effectively detect, understand, and contain cyber threats:

- Lacking – Unaware or unable to take effective action
- Minimal – Some basic structures in place to react if a problem should surface
- Satisfactory – Necessary structures in place to address current problems
- Advanced – Identifying and implementing structures that anticipate and address emerging problems
- N/A – Not applicable

After selecting a response for each statement, calculate your responses to understand how operational security corresponds to cybersecurity maturity of your organization.[7]

PEOPLE

1. Cybersecurity roles and responsibilities are coordinated to avoid duplication and are clearly defined in employee position descriptions

   - Example: IT Operations Manual, Employee Handbook, and Business Associates Agreements outline roles and responsibilities of all employees and third-parties

   ☐ Lacking ☐ Minimal ☐ Satisfactory ☐ Advanced ☐ N/A

   Source: ID.GV-2 (p. 26)

---

2. Employees, computer system security workers, and third-parties receive training for safeguarding systems and access to information, and preventing, detecting, and responding to cybers threat and attacks

   - Example: Employee Handbook, position requirements, employee training program including testing and exercises, signed contracts, memorandums of understanding, Business Associate Agreements

   ☐ Lacking ☐ Minimal ☐ Satisfactory ☐ Advanced ☐ N/A

   Source: ID.SC-4 (p. 28), PR.AT-1 (p. 31), PR.AT-2 (p. 31), PR.AT-3 (p. 31), PR.AT-4 (p. 31), PR.IP-11 (p. 35), DE.DP-1 (p. 40), RS.CO-1 (p. 41)

---

3. Employees and third-parties demonstrate understanding of the legal and regulatory requirements governing cybersecurity and their roles and responsibilities related to cyber threats and attacks

   - Example: HIPAA and HITECH, data security, patient privacy, and breach reporting

   ☐ Lacking ☐ Minimal ☐ Satisfactory ☐ Advanced ☐ N/A

   Source: ID.AM-6 (p. 24), ID.GV-3 (p. 26), ID.SC-1 (p. 28), ID.SC-5 (p. 29), PR.AT-5 (p. 31), RS.CO-4 (p. 41)

---

4. The organization shares with employees and third-parties the acceptable level of operational risk

   - Example: Risk assessment is completed and results included in employee training

   ☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

   Source: ID.RM-2 (p. 27)

---

5. Periodic monitoring and review of IT system activity log, such as Internet use, creation of new users, resetting of passwords, e-mail spam, file downloads, and use of portable external devices (e.g., flash drive)

   - Sample compliance: Audits of IT system logs and e-mail accounts

   ☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

   Source: DE.CM-3 (p. 39)

---

6. Information pertaining to cybersecurity processes, testing, threats, and attacks are received and shared with appropriate employees and third-parties

   - Example: Communication plan, cybersecurity plans, cyber incident reports, participation in online forums, stakeholder advisory groups, and other information sharing sessions

   ☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

   Source: ID.RA-2 (p. 26), DE.DP-4 (p.40), RS.CO-3 (p.41), RS.CO-5 (p. 41), RC.CO-3 (p.44)

---

7. Remote access is managed through formal approval and credentialing based on the role of the employee or third-party

   - Example: IT Systems Operation Manual outlines access requirements for each role, security procedures for encrypting data and using a virtual private network (VPN), remote desktop, or remote data base

   ☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

   Source: PR.AC-3 (p.29)

---

8. All users and devices undergo a standard approval process prior to use and all system identities and credentials are authenticated and managed by designated authorized employee

   - Example: IT Systems Operation Manual outlines requirements for usernames, passwords, application access, and authentication of credentials in line with risk

   ☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

   Source: PR.AC-1 (p.29), PR.AC-6 (p.30), PR.AC-7 (p.30)

---

9. User permissions and access privileges for IT systems, devices, software, and files are limited to only what is necessary to perform job functions

   - Example: Configuring user profiles and software based on role, key cards, and fobs limiting access to sensitive areas/materials

   ☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

   Source: PR.AC-3 (p.29), PR.AC-6 (p.30), PR.AC-7 (p.30), PR.PT-3 (p.37)

---

10. All employees and third-parties demonstrate adherence to established cybersecurity policies and regulations when using IT systems and software

- Example: Employee policies includes steps for non-compliance, and all agreements and contracts executed with third-parties detail responsibilities and termination clauses for non-compliance

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: PR.IP-5 (p.34)

PROCESSES

11. The mission, objectives, and activities of the organization have been established and communicated to employees and third-parties, as appropriate

- Example: Company Operation Manual, Employee Handbook, Memorandums of Understanding, Business Associate Agreements, contracts executed with third-parties, and Cyber Supply Chain Risk Management Plans

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: ID.BE-3 (p.25), ID.SC-1 (p.28)

12. The organization has a mapping of how information and data moves through IT systems and networks and has prioritized all activities, systems, software, and data that is essential for its operation

- Example: Workflow charts for communication and data transmission processes, evaluating of potential effects from an interruption in critical business operations and sharing results with employees and third-parties

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: ID. AM-3 (p.24), ID.AM-5 (p.24), ID.BE-4 (p.24), DE.AE-1 (p.37)

13. The organization has developed incident response and recovery plans that address cybersecurity and is able to execute plans during or after an event

- Example: Cybersecurity incident response, business continuity, disaster recovery, and cyber supply chain risk management plans are in place and updated

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: ID.BE-5 (p.25), ID.SC-5 (p.29), PR.IP-9 (p.35), PR.IP-10 (p.35), RS.RP-1 (p.40), RS.IM-1 (p.43), RS.IM-2 (p.43), RC.RP-1 (p.43), RC.IM-1 (p.43), RC.IM-2 (p.43)

---

14. Employees and third-parties understand the potential impact of a cyber-attack in delivering timely care to patients and ways to mitigate downtime with a cyber incident response plan

- Example: Business impact analysis, cybersecurity risk assessment, business continuity

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: ID.BE-1 (p.25); ID.BE-2 (p.25)

---

15. The organization identifies and documents known internal and external cyber threats, links these to results from cyber audits and testing, and uses this information to determine organization's risk level

- Example: Business impact analysis, and IT risk assessment report

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: ID.GV-4 (p.26), ID.RA-1 (p.26), ID.RA-4 (p.27), ID.RA.5 (p.27), ID.RA-3 (p.27), ID.RA-6 (p.27), ID.RM-1 (p.27), ID.RM-3 (p.28), PR.IP-12 (p.36), DE.AE-3 (p.38), RS.AN-4 (p.42), RS.AN-5 (p.42), RS.MI-3 (p.43)

---

16. Processes for secure data backup and recovery are implemented, documented, tested, and maintained

- Example: Disaster recovery planning

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: PR.IP-4 (p.34)

---

17. Cybersecurity policies are reviewed and tested to ensure defenses against cyber threats and alignment with industry best practices

- Example: Business impact and disaster recovery reports are generated and reviewed conducting mock cybersecurity drills, and lessons learned are communicated to employees and third-parties and documented in the IT Operations Manual

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: ID.SC-5 (p.29), PR.IP-7 (p.35), DE.DP-2 (p.40), DE.DP-3 (p.40), DE.DP-5 (p.40)

---

18. The organization shares information externally regarding selection, implementation, and use of technology to protect against cyber threats or attacks

- Example: Information sharing through participation in online forums, writing product reviews, developing third-party cyber supply chain risk management plans, and case studies

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: ID.SC-3 (p.28), ID.SC-4 (p.28), PR.IP-8 (p.35)

---

19. Notifications/alerts from detection systems, such as virus software, intrusion detection systems, or security management systems, are reviewed for suspicious activities and appropriate actions are taken to remediate potential threats

- Example: Risk assessment and business impact analysis to determine risk level by both probability and potential impact

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: DE.AE-2 (p.38), DE.AE-5 (p.38), RS.AN-1 (p.42), RS.AN.5 (p.42)

---

20. The organization contains cyber threats to minimize risk

- Example: Use of firewalls, VPNs, email security software, anti-malware software

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: RS.MI-1 (p.42), RS.MI-2 (p.43)

---

21. Information is collected, analyzed, and reported to relevant employees and third-parties following a cyberattack to understand the cause and impact the organization

- Example: Business impact analysis and disaster recovery reports

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: DE.AE-4 (p.38), RS.AN-2 (p.42), RS.AN-3 (p.42), RS.AN-5 (p.42)

---

22. A strategy is in place to manage public relations and repair the organization's reputation following a cyber threat or attack

- Example: Operations manual, disaster recovery plan, public relations strategy that include sharing remediation actions

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: RC.CO-1 (p.44), RC.CO.2 (p.44)

---

23. Criteria have been established to report cyber-attacks, monitor compliance with reporting, and remedy non-compliance with reporting policies

- Example: Disaster recovery plans, employee handbook and business associate agreements, trainings, documentation of counseling, and/or termination procedures for non-compliance

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: ID.SC-4 (p.28), ID.SC.5 (p.29), RS.CO-2 (p.41)

TECHNOLOGY

24. Physical devices, IT systems, and software that are both owned and not owned by the organization have been inventoried and recorded

- Example: Catalogue of all computers, mobile devices, electronic medical devices, printers, scanners, fax machines, copiers, any machines stored off site that are accessed virtually by the organization, programs installed on computers, and electronic health record systems

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: ID.AM-1 (p.24), ID.AM-2 (p.24), ID.AM-4 (p.24)

---

25. The IT systems, network, software, and third-party activity is monitored and scanned to detect potential unauthorized access and identify the source of the potential cyberattack

- Example: Vulnerability scans, penetration testing, and reviews of IT system access audit logs

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: ID.SC-4 (p.28), PR.PT-1 (p.36), PR.DS-6 (p.33), PR.DS.8 (p.33), DE.CM-1 (p.38), DE.CM-4 (p.39), DE.CM-5 (p.39), DE.CM-6 (p.39), DE.CM.7 (p.39), DE.CM-8 (p.39)

---

26. The physical environment outside of IT systems is restricted and monitored for unauthorized access

- Example: Security employees, key cards and fobs for access, and auditing of access and visitor logs

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: PR.AC-2 (p.29), DE.CM-2 (p.39)

---

27. All data that is stored, transmitted, or accessed by the organization is protected from unauthorized access

- Example: IT Operations Manual includes information on converting data to code (encrypting) and firewalls

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: ID.GV-1 (p.25), PR.DS-1 (p.32), PR.DS-2 (p.32), PR.DS-5 (p.32)

---

28. The IT systems network has the capacity to ensure data and software are always able to be accessed and used by authorized individuals

- Example: A calculator to determine the amount of data that can be transferred in one second, mechanisms such as failsafe, load balancing, and alternative hardware to prevent failure

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: PR.DS-4 (p.32), PR.PT-5 (p. 37)

---

29. IT systems used for testing and development are separated from systems that carry out daily operations of the organization

- Example: Internal firewalls, separate internet connections

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: PR.DS-7 (p.33)

---

30. Procedures for purchasing IT systems and software are established using a risk management process and agreed upon by stakeholders

- Example: IT Operations Manual outlines the process for, analysis, design, development, testing, installation, maintenance, evaluation, and disposal of IT systems and software

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: ID.SC-2 (p.28), PR.IP-2 (p.33)

---

31. Restrict changes to the IT system by limiting software installation and connection to external devices, as well as monitoring electronic communications and users of the system

- Example: Encryption, virus scans, monitoring of email and Internet use, limiting ability to install software to dedicated IT employees, blocking external devices (i.e., flash drives and smart phones) from connecting to a computer or network

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: PR.AC-5 (p.30), PR.IP-1 (p.33), PR.IP-3 (p.34), PR.PT-2 (p.36), PR.PT-4 (p.37)

---

32. Maintenance and repair of IT systems and software is documented and conducted by authorized individuals, vendors, and tools

- Example: List of approved vendors and tools, IT maintenance procedures in employee handbook and training

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: PR.MA-1 (p.36), PR.MA-2 (p.36)

---

33. IT systems and process for data removal, transfer, storage, and destruction are standard throughout the organization

- Example: IT Operations Manual and employee handbook and training addresses the removal, transfer, and storage of systems and data, and the process for overwriting, de-magnetizing, and shredding data

☐ **Lacking** ☐ **Minimal** ☐ **Satisfactory** ☐ **Advanced** ☐ **N/A**

Source: PR.DS-3 (p.32), PR.IP-6 (p.34)

CYBERSECURITY MATURITY RESULTS

Calculate the total number of response options selected for all self-evaluation statements. Then review the corresponding maturity level on the right, which is an indicator of preparedness to detect, understand, and contain cyber incidents and a potential breach. Maturity levels are based on a cybersecurity maturity model that has been validated through extensive research.[8] Results can be used by organizations to identify areas for improvement. In general, higher levels of maturity correspond to better operational security; lower levels of maturity should be prioritized to identify and implement cybersecurity improvements in people, processes, and technology.

Response Option	Total Number Selected	Cybersecurity Maturity Level
Lacking	#	Unprepared – Lacking necessary information to take effective action; unaware or unable to respond to current or emerging issues
Minimal	#	Reactive – Basic platforms and structures in place to react to business requirements; unable to proactively prevent problems from arising
Satisfactory	#	Proactive – Platforms, structures, and processes in place to proactively address current issues and challenges
Advanced	#	Anticipatory – Platforms, structures, and processes in place necessary to address future issues and challenges
N/A	#	N/A – Not applicable

MATURITY LEVELS

More information on the maturity levels:[9]

- **Unprepared**: Lacking people (cybersecurity personnel), technology (anti-virus software, firewalls, etc.), processes (e.g., regular cybersecurity awareness training, incident response plans) to deal with cyber threats.
- **Reactive:** People, technology, and processes in place to handle cyberattacks after they occur.
- **Proactive:** People, technology, and processes in place to protect against foreseeable threat (e.g., assigns least required access privileges needed to perform specific tasks, security configurations continuously evaluated, etc.)[10]
- **Anticipatory:** People, technology, and processes able to protect against cyber threats that could emerge (e.g., looking into potential impacts of new technology such as blockchain).

KEY TERMS

A full list of cybersecurity terms and definitions is available at: csrc.nist.gov/glossary

RESOURCES

1. ***Baldrige Cybersecurity Excellence Builder***, NIST March 2019. Available at: www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative.

2. ***Security Risk Assessment Tool***, HealthIT.gov. Available at: www.healthit.gov/providers-professionals/security-risk-assessment-tool

3. ***Framework for Improving Critical Infrastructure Cybersecurity Version 1.1,*** NIST April 2018. Available at: nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

4. ***Security and Privacy Controls for Federal Information Systems and Organizations***, NIST Special Publication 800-53 Revision 5. Available at: nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

5. ***HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework***, Department of Health and Human Services Office for Civil Rights. Available at: www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf

6. ***Cybersecurity Maturity Model Lays out Four Readiness Levels***, Tech Target. Available at: www.techtarget.com/searchsecurity/tip/Cybersecurity-maturity-model-lays-out-four-readiness-levels

ABOUT MHCC

The MHCC is an independent regulatory agency whose mission is to plan for health system needs, promote informed decision-making, increase accountability, and improve access in a rapidly changing health care environment by providing timely and accurate information on availability, cost, and quality of services to policy makers, purchasers, providers and the public. The MHCC is responsible for advancing health information technology statewide and fostering innovation in a way that balances the need for information sharing with the need for strong privacy and security policies.

ACKNOWLEDGEMENTS

The MHCC appreciates the contribution made by members of the Maryland Hospital Association, MedChi, The Maryland State Medical Society, LifeSpan Network, Maryland Association of Community Health Centers, and Health Facilities Association of Maryland in developing and testing this questionnaire.

QUESTIONNAIRE FEEDBACK

The MHCC would greatly appreciate your feedback on the utility of this questionnaire by responding to a brief survey at the following link: www.surveymonkey.com/r/CSSAToolFeedback.

Endnotes

[1] Ready.gov. *Cybersecurity*. Available at: www.ready.gov/cybersecurity
[2] NIST was established by Congress in 1901 to create a measurement infrastructure for technology. A wide variety of industries, including health care, rely on NIST technology, measurement, and standards. More information is available at: www.nist.gov/about-nist.
[3] The Cybersecurity Self-Assessment Tool uses the functions, categories, and subcategories developed by NIST. Descriptions in this document contain language used in the "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1" developed by NIST. A copy of the document can be accessed at: nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
[4] The NIST CSF was first released in February 2014. It was then updated in April 2018 to reflect industry feedback, which includes clarifying cybersecurity measurement language and tactics for improving security within the supply chain. In general, updates in Version 1.1 are non-substantive and intended to be compatible with the existing Version 1.0.
[5] NIST, *The Five Functions*. Available at: www.nist.gov/cyberframework/online-learning/five-functions.
[6] Page numbers represent document pages, not page numbers indicated by Adobe® PDF Reader.
[7] TechTarget, *Cybersecurity Maturity Model Lays out Four Readiness Levels,* January 2019. Available at: techtarget.com/searchsecurity/tip/Cybersecurity-maturity-model-lays-out-four-readiness-levels.
[8] *Ibid.*
[9] See n. 7, *Supra.*
[10] Crowdstrike. *Zero Trust Security Explained: Principals of the Zero Trust Model*, May 2021. Available at: www.crowdstrike.com/cybersecurity-101/zero-trust-security/.